Amendments to the claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-147. (Cancelled).

148. (New) A method, comprising:

receiving, using one or more processors, a resource library, wherein the resource library includes an embedded text string specifying one or more use terms corresponding to the resource library, and wherein the resource library includes an embedded unique key mathematically derived from the text string using a private key;

separately receiving a copy of the text string and a copy of the unique key and embedding the copy of the text string and the copy of the unique key within an application;

running the application, wherein running includes extracting the text string and the unique key from the resource library, verifying the authenticity and state of the text string using the unique key, and determining whether the application is authorized to use the resource library by examining the one or more terms specified in the extracted text string and the one or more terms specified in the copy of the text string embedded within the application, wherein when the one or more terms are satisfied, the application is authorized to use the resource library; and

unlocking the resource library when the application is authorized, wherein unlocking includes allowing the authorized application to access the resource library.

149. (New) The method of claim 148, wherein verifying the state includes determining that the text string does not include an unauthorized modification.

150. (New) The method of claim 148, wherein the application is authorized because a site term is satisfied.

151. (New) The method of claim 148, wherein when a term is not satisfied, an error message is generated, the application is not authorized, and access to the resource library is denied.

152. (New) The method of claim 148, wherein the unique key includes a digital signature, and wherein the digital signature uses a message digest generated by passing the text string through a one-way encryption process.

153. (New) The method of claim 152, wherein the one-way encryption process is a hashing routine.

154. (New) The method of claim 152, wherein the digital signature is verified by performing an algorithmic process using a public key.

155. (New) The method of claim 148, wherein the resource library is an application program interface (API).

156. (New) The method of claim 148, wherein the resource library is a Java applet.

157. (New) A system, comprising:

one or more processors;

one or more computer-readable storage mediums containing instructions configured to cause the one or more processors to perform operations, including:

receiving a resource library, wherein the resource library includes an embedded text string specifying one or more use terms corresponding to the resource library, and wherein the resource library includes an embedded unique key mathematically derived from the text string using a private key;

separately receiving a copy of the text string and a copy of the unique key and embedding the copy of the text string and the copy of the unique key within an application;

running the application, wherein running includes extracting the text string and the unique key from the resource library, verifying the authenticity and state of the text string using the unique key, and determining whether the application is authorized to use the resource library by examining the one or more terms specified in the extracted text string and the one or more terms specified in the copy of the text string embedded within the application, wherein when the one or more terms are satisfied, the application is authorized to use the resource library; and

unlocking the resource library when the application is authorized, wherein unlocking includes allowing the authorized application to access the resource library.

158. (New) The system of claim 157, wherein verifying the state includes determining that the text string does not include an unauthorized modification.

159. (New) The system of claim 157, wherein the application is authorized because a site term is satisfied.

160. (New) The system of claim 157, wherein when a term is not satisfied, an error message is generated, the application is not authorized, and access to the resource library is denied.

161. (New) The system of claim 157, wherein the unique key includes a digital signature, and wherein the digital signature uses a message digest generated by passing the text string through a one-way encryption process.

162. (New) The system of claim 161, wherein the one-way encryption process is a hashing routine.

163. (New) The system of claim 161, wherein the digital signature is verified by performing an algorithmic process using a public key.

164. (New) The system of claim 157, wherein the resource library is an application program interface (API).

165. (New) The system of claim 157, wherein the resource library is a Java applet.

166. (New) A computer-program product, tangibly embodied in a machine-readable storage medium, including instructions configured to cause a data processing apparatus to:

receive a resource library, wherein the resource library includes an embedded text string specifying one or more use terms corresponding to the resource library, and wherein the resource library includes an embedded unique key mathematically derived from the text string using a private key;

separately receive a copy of the text string and a copy of the unique key and embedding the copy of the text string and the copy of the unique key within an application;

run the application, wherein running includes extracting the text string and the unique key from the resource library, verifying the authenticity and state of the text string using the unique key, and determining whether the application is authorized to use the resource library by examining the one or more terms specified in the extracted text string and the one or more terms specified in the copy of the text string embedded within the application, wherein when the one or more terms are satisfied, the application is authorized to use the resource library; and

unlock the resource library when the application is authorized, wherein unlocking includes allowing the authorized application to access the resource library.

167. (New) The computer-program product of claim 166, wherein verifying the state includes determining that the text string does not include an unauthorized modification.

168. (New) The computer-program product of claim 166, wherein the application is authorized because a site term is satisfied.

169. (New) The computer-program product of claim 166, wherein when a term is not satisfied, an error message is generated, the application is not authorized, and access to the resource library is denied.

170. (New) The computer-program product of claim 166, wherein the unique key includes a digital signature, and wherein the digital signature uses a message digest generated by passing the text string through a one-way encryption process.

171. (New) The computer-program product of claim 170, wherein the one-way encryption process is a hashing routine.

172. (New) The computer-program product of claim 170, wherein the digital signature is verified by performing an algorithmic process using a public key.

173. (New) The computer-program product of claim 166, wherein the resource library is an application program interface (API).

174. (New) The computer-program product of claim 166, wherein the resource library is a Java applet.